(ISC)²®

Chapter 3 Resource

Access Control Concepts

Chapter Summary

In this chapter, we described who gets access to what, why access is necessary, and how that access is managed. Access is based on three elements: subjects (who), objects (what), and rules (how and when). Trustworthiness and the need for access also determine access.

We also discussed defense in depth (an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization) and how it applies to the types of access control (physical, logical/technical, and administrative) that every information security professional should be familiar with. At the same time, we stressed the importance of the Principle of Least Privilege (users should only have the minimum access necessary to accomplish their job).

We then discussed Privileged Access Management and how it relates to risk and the CIA Triad: it reduces risk by allowing admin privileges to be used only when needed, provides confidentiality by limiting the need for administrative access that is used during routine business, ensures integrity by only allowing authorized administrative access during approved activities, and confirms availability by providing administrative access when needed. We also differentiated between a Regular User Account and a Privileged User Account.

We further discussed segregation of duties, two-person integrity, and how users are provisioned, from being hired to being terminated. We then explored physical and logical access controls and how they are combined to strengthen the overall security of an organization. Physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles and alarms. Logical access controls (also called technical controls) can be configuration settings or parameters stored as data, managed through a software graphical user interface (GUI), or they can be hardware settings done with switches, jumper plugs or other means.

We concluded the chapter discussing three logical access controls: DAC, MAC, and RBAC. Discretionary access control (DAC) is a specific type of access control policy that is controlled by the owner of the resource and enforced at the subject level over objects in an information system. A mandatory access control (MAC) policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system. Role-based access control (RBAC), as the name suggests, sets up user permissions based on roles.

Module Names

Module 1: Understand Access Control Concepts

Module 2: Understand Physical Access Controls

Module 3: Understand Logical Access Controls

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Access Control Concepts	3.1, 3.1.3, 3.1.5, 3.2, 3.2.1, 3.2.2, 3.2.5
2	Understand Physical Access Controls	3.1, 3.1.1, 3.1.2
3	Understand Logical Access Controls	3.2, 3.2.3, 3.2.4, 3.2.5

Learning Objectives

After completing this chapter, the participant will be able to:

- Select access controls that are appropriate in a given scenario.
- Relate access control concepts and processes to given scenarios.
- Compare various physical access controls.
- Describe logical access controls.
- Practice the terminology of access controls and review concepts of access controls.

Chapter Takeaways

Module 1: Understand Access Control Concepts

Access is based on three elements:

- Subjects (Who)
- Objects (What)
- Rules (How and When)

Defense in Depth

- An information security strategy that integrates people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
- Applies multiple countermeasures in a layered fashion to fulfill security objectives.
- Should be implemented to prevent or deter a cyberattack, but it cannot guarantee that an attack will not occur.

Privileged Access Management

- Reduces risk by allowing admin privileges to be used only when needed.
- Provides confidentiality by limiting the need for administrative access that is used during routine business.
- Ensures integrity by only allowing authorized administrative access during approved activities.
- Confirms availability by providing administrative access when needed.

How Users are Provisioned

- New employee – account created
- “Onboarding” – creating an account (or cloning a baseline account) for a new employee
- Changed position – account modified
- Temporary leave of absence – account disabled
- Separation of employment – account deleted
- “Offboarding” – deleting an account (or disabling then deleting an account) for a terminated employee

Chapter Takeaways (Continued)

Module 2: Understand Physical Access Controls

Examples of physical access controls:

- Security guards
- Fences
- Motion detectors
- Locked doors/gates
- Sealed windows
- Lights
- Cable protection
- Laptop locks
- Badges
- Swipe cards
- Guard dogs
- Cameras
- Mantraps/turnstiles
- Alarms

Log terminology:

- Log anomaly
- Log consolidation
- Log retention

Module 3: Understand Logical Access Controls

Logical access control types:

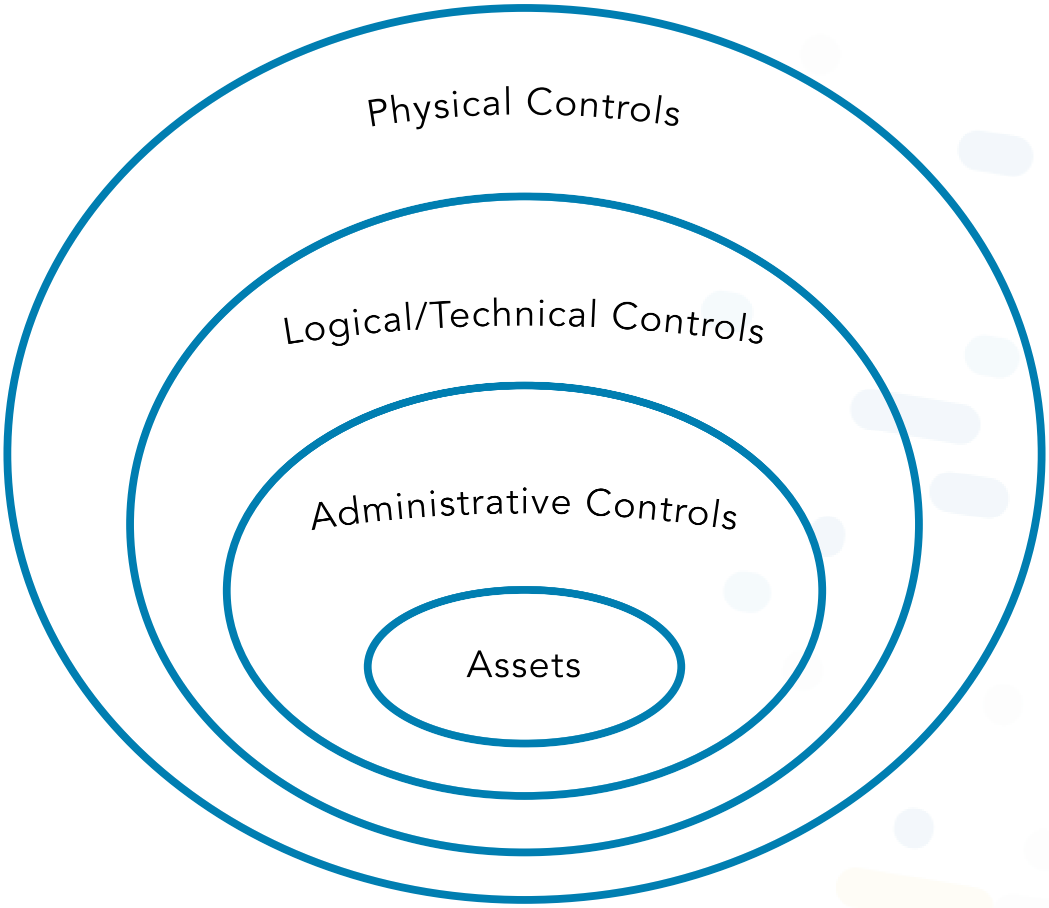
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

Examples of logical access controls:

- Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI)
- Hardware settings done with switches, jumper plugs or other means

Graphics

Defense in Depth



Chapter Terms and Definitions

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. NIST SP 1800-15B

Crime Prevention through Environmental Design (CPTED)

An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.

Defense in Depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. Source: NIST SP 800-53 Rev 4

Discretionary Access Control (DAC)

A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. NIST SP 800-192

Encrypt

To protect private information by putting it into a form that can only be read by people who have permission to do so.

Firewalls

Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.

Insider Threat

An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. NIST SP 800-32

iOS

An operating system manufactured by Apple Inc. Used for mobile devices.

Layered Defense

The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.

Linux

An operating system that is open source, making its source code legally available to end users.

Log Anomaly

A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.

Logging

Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks. NIST SP 1800-25B.

Logical Access Control Systems

An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization. NIST SP 800-53 Rev.5.

Mandatory Access Control

Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Mantrap

An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

Object

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See subject. Source: NIST SP 800-53 Rev 4

Physical Access Controls

Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Principle of Least Privilege

The principle that users and programs should have only the minimum privileges necessary to complete their tasks. NIST SP 800-179

Privileged Account

An information system account with approved authorizations of a privileged user. NIST SP 800-53 Rev. 4

Ransomware

A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid.

Role-based access control (RBAC)

An access control system that sets up user permissions based on roles.

Rule

An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

Segregation of Duties

The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties.

Subject

Generally an individual, process or device causing information to flow among objects or change to the system state. Source: NIST SP800-53 R4

Technical Controls

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Turnstile

A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

Unix

An operating system used in software development.

User Provisioning

The process of creating, maintaining and deactivating user identities on a system.